REMARKS

Initially, Applicant expresses appreciation to the Examiners for the courtesies extended in the recent telephonic discussion held with Applicant's representatives. The amendments and remarks presented herein are consistent with the content of that discussion. Accordingly, entry of this amendment is respectfully requested.

The Office Action, mailed December 15, 2006, considered and rejected claims 1-12, 14-22 and 24-29. Claims 1-12, 14-22 and 24-29 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite.[1] Claims 1-12, 14-22 and 24-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *CERT-Advisory* (CERT CC, "CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests" in view of *CERT* (CERT CC, "Understanding Malicious Content Mitigation for Web Developers," and further in view of *Wheeler* ("Secure Programming for Linux and Unix HOWTO").[2]

By this paper, claims 1, 4, 8, 18 and 27 have been amended, and no claims have been cancelled or added.[3] Accordingly, following this paper, claims 1-12, 14-22 and 24-29 remain pending, of which claims 1, 14 and 24 are the only independent claims at issue.

As reflected in the above claim listing, Applicant's claims are generally directed to methods and computer program products for mitigating a cross-site scripting attack. As recited in claim 1, for example, a method to mitigate such attacks includes maintaining, at a server, a list of active markers. A request is also received from a user computer and includes data derived from an outside source. A determination is made whether the request includes a marker of active content as identified in the list of active markers. Thereafter, the server refrains from serving a response to any portion of the request if the request includes the marker of active content. The user is then informed that a marker of active content from the list of active markers on the server has been discovered in the request and is requested to resubmit a request. If the resubmitted

---

[1] Although Applicant does not necessarily agree with the assertions made regarding the claims being indefinite, Applicant submits that particularly in view of the claim amendments, this rejection is now moot. In particular, Applicant has clarified that a first request includes safe and outside data portions. After determining that the outside data portions include markers of active content, a request is made that the user resubmit a request, to which a response is served if the resubmitted request does not include markers of active content.

[2] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should the need arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[3] Support for the claim amendments can be found in the express, implied and inherent disclosure of Applicant's original application, including at least the disclosure in paragraphs 6, 7 and 24-31of the original application.

request is clean of active markers, such as those inserted by an outside source, a response to the resubmitted request is served.

Claim 8 is directed to a similar method in which an HTTP request is made and checked for script constructs, while claim 24 recites a computer program product generally corresponding to the method of claim 8.

As discussed with the Examiner, while *CERT-Advisory*, *CERT*, and *Wheeler* generally relate to preventing damage from cross-scripting attacks, Applicant respectfully submits that they fail to disclose or suggest Applicant's invention. For example, among other things, the cited references fail to disclose or suggest wherein upon determining that a marker of active content exists, the server refrains from serving a response to any portion of the request, as recited in combination with the other claim elements. Indeed, when reviewed either alone or in their entirety, the cited references appear to teach the opposite in that a request from a user computer is filtered to remove malicious code, while still passing through and executing the non-malicious code.

As expressly disclosed in *CERT-Advisory* and *CERT*, a request received from a client is not aborted, and continues to be processed, at least in part, even where it contains malicious code. For example, *CERT-Advisory* generally discusses the problem associated with malicious code from a cross-site scripting attack. (pp. 1-2). To address such problems, *CERT-Advisory* notes that web site developers can prevent such attacks by allowing only a limited character set or by filtering data during generation of the output page. (p. 5, ¶ 3-6). Thus, *CERT-Advisory* discloses that while filtering for script characters is performed, an output page is generated. For additional details on encoding and filtering, however, *CERT-Advisory* refers to the *CERT* reference.

CERT adds to the discussion in *CERT-Advisory* regarding methods for avoiding damage due to cross-site scripting attacks. As explained in *CERT*, damage from such attacks can be minimized by filtering specific characters out of web pages that contain both text and HTML markup. (pp. 1, 4). For instance, a web page request may be filtered either during the data input or data output process to ensure that all dynamic content is filtered. (p. 4, ¶ 4). Thus, *CERT* discloses that dynamic content is affected, by does not disclose that serving of any response to static content is affected.

Furthermore, *CERT* provides three examples of code to perform the requested filtering. (p. 4). For instance, in a JavaScript example, a string of characters in a request is examined for particular characters (e.g., < > " ' % ; ( ) & +). If any of these characters is found, it is replaced by a null value. The string of characters is then returned which results in the bad character being removed, while any characters not identified as "bad" characters are still passed through. Similar examples are disclosed for C++ and PERL and, in each case, bad characters are filtered out, but "good" characters are still returned. (*See* p. 5, *et seq.*). Accordingly, in each example, although malicious characters are removed, non-malicious characters are still processed and returned to the user.

Accordingly, *CERT-Advisory* and *CERT* disclose that characters within a request are filtered and replaced, and expressly disclose that even in the presence of such characters, the request is still processed and a response served. In other words, when a request is received, *CERT-Advisory* and *CERT* disclose that while "bad" characters in a request are filtered and removed, a portion of the request—namely the "good" characters—continues to be processed. Applicant respectfully submits that this is in contrast to Applicant's claimed invention in which rather than serving a response to portions of a request that are free of markers of active content, Applicant's method refrains from serving a response to <u>any</u> portion of the request. Further, inasmuch as such teachings are directly contrary to the recited limitations, Applicant respectfully submits that threw would also be no motivation to combine such references with another reference purportedly teaching aborting or otherwise refraining from serving a response to every portion of a request, as recited in combination with the other claim elements.

Applicant also respectfully submits that the *Wheeler* reference fails to remedy the deficiencies of *CERT-Advisory* and *CERT*. Indeed, *Wheeler* makes express reference to, and approval of, the systems employed in *CERT-Advisory* and *CERT* when describing how to solve the problem of cross-site scripting. (*See* §§ 4.10, 6.15-6.15.2.2, 8.5).

For example, *Wheeler* expressly approves of the filtering method of *CERT-Advisory* and *CERT* and notes that to make a program safe, the "<u>output</u> must be filtered (so characters that can cause this problem are removed), encoded..., or validated." (§ 6.15.2). Such filtering, as described by *Wheeler* entails removing the special or "bad" characters, while leaving valid characters unaffected. (§ 6.15.2.2). Thus, malicious characters are removed while non-malicious characters continue to be passed through.

In addition, or in the alternative, *Wheeler* describes that characters may alternatively be encoded. (§ 6.15.2.3) For instance, a '<' may be encoded as '<', '&' becomes '&', and the like. Thus, the potentially malicious characters are encoded. *Wheeler* fails, however, to have any teaching regarding encoding non-malicious portions of the request. Indeed, *Wheeler* expressly notes that only the portions where user-input is under the control of an untrusted user need be screened, such that non-malicious portions of the trusted user would continue to be processed without encoding. (§ 4).

In another example, *Wheeler* discloses that character encoding in the output can be established so as to prevent malicious codes. (§ 8.5). Again, however, such a disclosure relies on there being output to generate and provide as a response. In other words, in Applicant's claims, there can be no output sent to the response as the server retrains from serving the response to any portion of the request where the request includes active markers. In contrast, *Wheeler* expressly teaches that even if the code is malicious, an output is generated and provided; however the response is safe because the charset had been previously specified to limit malicious characters.

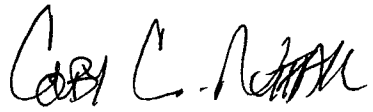
Accordingly, in contrast to Applicant's claimed invention, in which a server refrains from serving a response to any portion of a request that includes both safe data and data from an outside source, each of *CERT-Advisory*, *CERT*, and *Wheeler* expressly disclose that if a malicious code is received, the malicious code is neutralized while the non-malicious portion is processed. Thus, the cited references, whether considered alone or in combination, fail to disclose each and every claim limitation of Applicant's invention.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 14 day of March, 2007.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
COLBY C. NUTTALL
Registration No. 58,146
Attorneys for Applicant
Customer No. 047973

RDN:JCJ:CCN:gd
GD0000001611V001